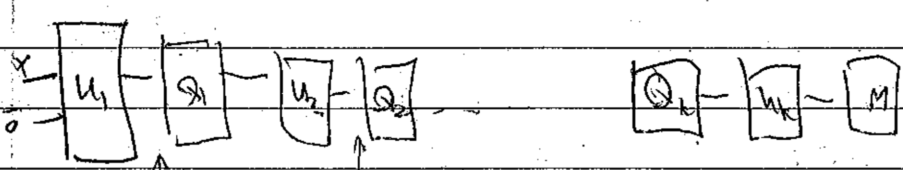
BBB V.99

הוכחה שאי אפשר יותר מהר!

הוכחה שאי אפשר לעבור את הזמן של search עם פחות מ $\sqrt{N}$ שאילתות?

נניח יש לנו אלגוריתם עם k שאילתות — הפעלות כלומר



$\varphi^{(0)}$ $\varphi^{(1)}$

אם נבצע אלגוריתם, עם $f \equiv 0$, נקבל סדרה של מצבים. נסמן את מצב הקיום לפני שאילתה ה-t ב-

$$\varphi^{(0)}, \varphi^{(1)}, \varphi^{(2)}, \ldots, \varphi^{(k)}$$

נסמן

$$\varphi^{(t)} = \sum_x \alpha_x^{(t)} |x, \xi_{x,t}\rangle$$

בנורמה 1

אינטואיטיבית: $|\alpha_x^{(t)}|^2$ — ההסתברות שנשאל על x בזמן t.

יודעים ש

$$\sum_t \sum_x |\alpha_x^{(t)}|^2 = T$$

לכן יש x_0 כך ש

$$\sum_t |\alpha_{x_0}^{(t)}|^2 \le \frac{T}{N}$$

ולכן

$$\sum_t |\alpha_{x_0}^{(t)}| \le \sqrt{\sum_t |\alpha_{x_0}^{(t)}|^2}\,\sqrt{T} \le \frac{T}{\sqrt{N}}$$

אינטואיציה: אם $T \ll \sqrt{N}$, האלגוריתם לא שואל מספיק על x_0

לכן אם נשנה את f ל g כך ש

$$g(x) = \begin{cases} 1 & x = x_0 \\ 0 & \text{אחרת} \end{cases}$$

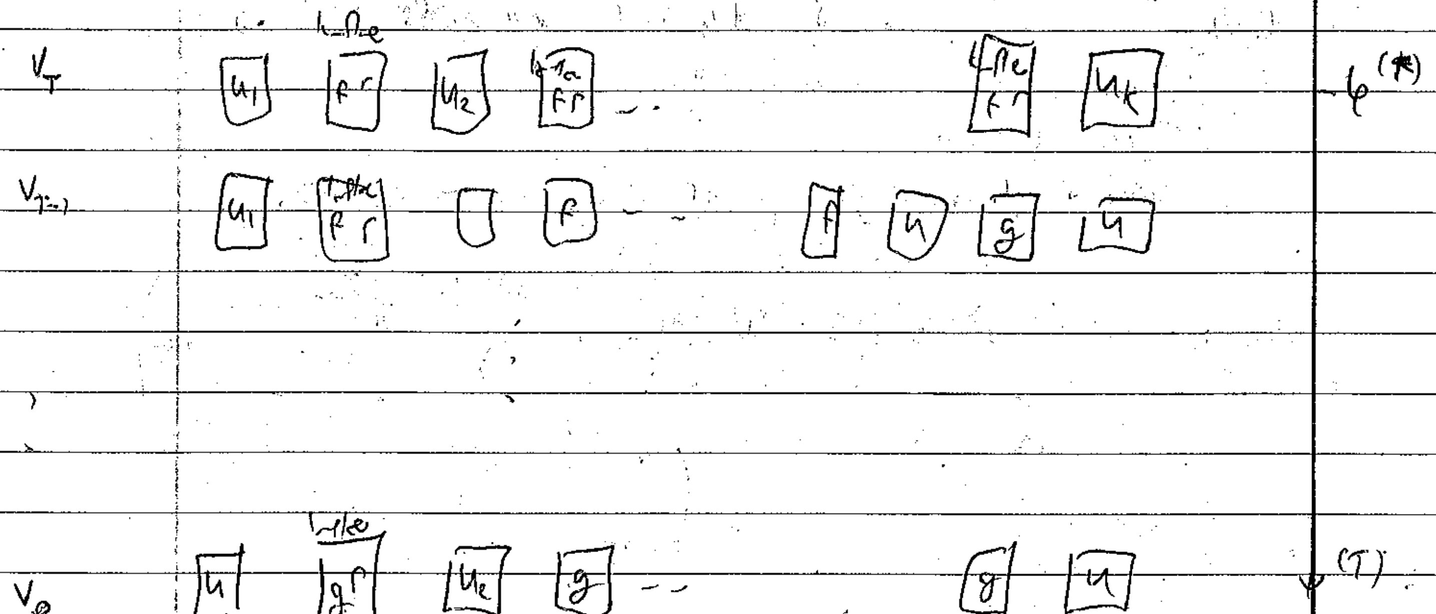
לא נוכל להבחין בין f ו g והאלגוריתם יטעה בהכרח.

שיעור 10

(1)

נתון ה- $\psi^{(t)}, \dots, \psi^{(0)}$ של מצבי האלגוריתם כשעושים שאילתות ל-g
מהו $\|\psi^{(T)} - \varphi^{(T)}\|$?

נעשה טיעון Hybrid



$\|V_T - V_0\| \le \sum_{i=1}^{T} \|V_{i+1} - V_i\|$

מהו $\|V_{i+1} - V_i\|$? – ה-i הפעולות הראשונות זהות, ואז מגיעים ל- $\varphi^{(i)}$
במקרה 1 מפעילים שאילתה f ומגיעים ל- $\varphi^{(i+1)}$
" 2 " " g " $\bar{\varphi}$

מקבלים שההפרש רק ב- V_0 והוא $\|Q_f \varphi^{(i)} - Q_g \varphi^{(i)}\|$

$\le 2|\alpha^{(i)}_{x_0}|$

ואח"כ מפעילים אותן U, נקרא להם W

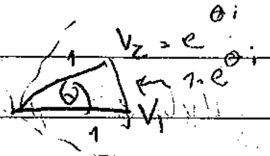
$\|WV_1 - WV_2\| = \|W(V_1 - V_2)\| \le \|W\| \cdot \|V_1 - V_2\| \le \|V_1 - V_2\|$

לסיכום $\|V_T - V_0\| \le 2\sum_{i=1}^{T} |\alpha^{(i)}_{x_0}| \le \frac{2T}{\sqrt{N}}$

מה טוב אפשר להבדיל בין 2 מצבים קרובים?

נניח v_1, v_2 ש- $\|v_1 - v_2\| \le \delta$.

הערה כי מתקיים

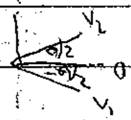


$\frac{\delta}{\sin\theta} = \frac{1}{\sin(\frac{\pi}{2}-\frac{\theta}{2})}$

$$\delta = \|v_1 - v_2\| = 2\sin\frac{\theta}{2}$$

$$\sin\frac{\theta}{2} = \frac{\delta}{2}$$

ראינו שהכי טוב שאפשר להבחין [illegible] θ



$$|v_2\rangle\langle v_2| - |v_1\rangle\langle v_1| = \begin{pmatrix} \cos^2\frac{\theta}{2} & -\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) \\ -\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) & \sin^2\frac{\theta}{2} \end{pmatrix} - \begin{pmatrix} \cos^2\frac{\theta}{2} & + \\ + & \sin^2\frac{\theta}{2} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \sin(\theta) \\ \sin(\theta) & 0 \end{pmatrix}$$

$\lambda_2 = -\lambda_1$ $\qquad -\lambda_1^2 = \lambda_1\lambda_2 = -\sin^2(\theta)$

$\lambda_{1,2} = \pm\sin(\theta)$ $\qquad |\rho_1 - \rho_2|_{tr} = |\lambda_1| + |\lambda_2| = 2\sin\theta$

ולכן [illegible] $\left(\frac{1}{2} - \frac{|\rho_1-\rho_2|}{4}, \; \frac{1}{2} + \frac{|\rho_1-\rho_2|}{4}\right)$

ולכן נקבל $\sin\theta = \frac{|\rho_1-\rho_2|}{2}$.

$|\sin\theta| = 2|\sin\frac{\theta}{2}||\cos\frac{\theta}{2}| \le |2\sin\frac{\theta}{2}| = \delta$ □.

ולכן, אם רוצים הסתברות הצלחה קבועה צריך

$$\frac{2T}{\sqrt{N}} = \Theta(1)$$

$$\boxed{T = \Theta(\sqrt{N})}$$ □

לסיכום שלא ניתן לפתור את NP בקוונטי BBBV.

מה זה אומר ומה לא.

(3)